

AMENDMENTS TO THE CLAIMS

1 1. (Currently Amended) A policy-based network security management system, the
2 system comprising:
3 a security management controller comprising one or more processors;
4 a computer-readable medium carrying one or more sequences of instructions for
5 policy-based network security management, wherein execution of the one or
6 more sequences of instructions by the one or more processors causes the one
7 or more processors to perform the steps of:
8 receiving a set of data regarding a user of a network, wherein the set of data is
9 a first set of data that is collected over a first duration of time;
10 receiving a second set of data that is collected over a second duration of time,
11 wherein the first duration of time is shorter than the second duration of
12 time;
13 ~~assessing creating and storing a risk level of the user harming the network~~
14 based on the second set of data, wherein the second duration of time is
15 sufficient to collect historical data regarding past malicious activities
16 of the user, ~~and wherein the risk level is a discrete value representing a~~
17 ~~long-term measurement of the likelihood of the user harming the~~
18 ~~network;~~
19 ~~assessing creating and storing a current alert level based on the first set of~~
20 data, wherein the first duration of time is of a length appropriate for
21 assessing current activities of the user, ~~and wherein the current alert~~
22 ~~level is a discrete value representing a current measurement of the~~
23 ~~likelihood of the user negatively affecting the network;~~
24 automatically deciding on a course of action based on ~~at least one~~ of the risk
25 level and the current alert level, wherein the course of action may be
26 adverse to the user although the current alert level is insufficient to
27 establish whether the user is performing a malicious action; and
28 sending signals to one or more network elements in the network to implement
29 the course of action.

1 2. (Original) The system of Claim 1, wherein the set of data includes at least one or
2 more alerts related to the user.

1 3. (Original) The system of Claim 1, wherein the signals include multiple alerts
2 generated by multiple users; and the system further comprising sequences of
3 instructions for correlating the multiple alerts to the multiple users.

1 4-5. (Canceled)

1 6. (Previously Presented) The system of Claim 1, further comprising sequences of
2 instructions for performing the steps of:
3 receiving signals related to an external source including at least an alert assessment
4 relevant to the network as a whole; and
5 creating and storing a current alert level value based on the alert assessment.

1 7. (Original) The system of Claim 1, further comprising sequences of instructions
2 for performing the steps of:
3 receiving signals carrying performance information related to a health level of the
4 network; and
5 determining the course of action based at least in part on the set of data and the
6 performance information.

1 8. (Original) The system of Claim 1 further comprising:
2 a plurality of routers for routing information sent by users and servers to a variety of
3 destinations;
4 a subscriber management system for managing a network;
5 a controller for executing the sequences of instructions;
6 a network element for generating input for the set of data; and
7 sequences of instructions for sending signals to the network elements.

1 9. (Currently Amended) A computer-readable tangible storage medium carrying one or
2 more sequences of instructions for providing policy-based network security
3 management, wherein execution of the one or more sequences of instructions by one
4 or more processors causes the one or more processors to perform the steps of:
5 receiving signals carrying network performance information regarding health of a
6 network and resource performance information regarding health of resources
7 used by the network;
8 assessing a health level based on the network performance information and the
9 resource performance information;
10 wherein the network performance information, on which the health level is based,
11 comprises at least one of packet latency information, jitter information, packet
12 loss probability (PLP) information, network throughput information, average
13 network downtime information, mean time to repair information, and mean
14 time between failure information;
15 wherein the resource performance information, on which the health level is based,
16 comprises at least one of DHCP server utilization information and ARP table
17 utilization information; and
18 sending signals carrying information affecting use of the network based on at least the
19 health level.

1 10. (Previously Presented) A computer-readable medium as recited in Claim 9,
2 further comprising the steps of:
3 receiving signals related to one or more alerts;
4 associating with a user at least the one or more alerts within a current alert dataset that
5 establishes a current alert level for the user.

1 11. (Original) A computer-readable medium as recited in Claim 9, further comprising
2 the step of establishing a user alert.

1 12. (Original) A computer-readable medium as recited in Claim 9, further comprising
2 the steps of:

3 receiving signals related to one or more alerts;
4 associating with a user at least the one or more alerts within a historical dataset of
5 alert related information that establishes a user risk level for the user.

1 13. (Previously Presented) A computer-readable medium as recited in Claim 9,
2 wherein the step of sending signals further comprises the steps of:
3 deciding on a course of action based on at least a user risk level, a current alert level,
4 and the health level,
5 wherein the information affecting the use of the network is based on at least the
6 course of action.

1 14. (Previously Presented) A computer-readable medium as recited in Claim 13,
2 wherein the deciding step includes at least:
3 determining the user risk level and determining the current alert level,
4 wherein the information affecting the use of the network is based on at least the user
5 risk level, the current alert level, and the health level.

1 15. (Previously Presented) A policy-based network security management system,
2 the system comprising:
3 a security management controller comprising one or more processors; and
4 the computer-readable medium of Claim 9.

1 16. (Currently Amended) A method of providing policy-based network security
2 management, comprising the steps of:
3 receiving a set of data regarding a user of a network, wherein the set of data is a first
4 set of data that is collected over a first duration of time;
5 receiving a second set of data that is collected over a second duration of time, wherein
6 the first duration of time is shorter than the second duration of time;
7 assessing creating and storing a risk level of the user harming the network based on
8 the second set of data, wherein the second duration of time is sufficient to
9 collect historical data regarding past malicious activities of the user, and

10 wherein the risk level is a discrete value representing a long-term
11 measurement of the likelihood of the user harming the network;
12 assessing creating and storing a current alert level based on the first set of data,
13 wherein the first duration of time is of a length appropriate for assessing
14 current activities of the user, and wherein the current alert level is a discrete
15 value representing a current measurement of the likelihood of the user
16 negatively affecting the network;
17 automatically deciding on a course of action based on ~~at least one~~ of the risk level and
18 the current alert level, wherein the course of action may be adverse to the user
19 although the current alert level is insufficient to establish whether the user is
20 performing a malicious action; and
21 sending signals to one or more network elements in the network to implement the
22 course of action.

1 17. (Original) The method of Claim 16 wherein the set of data includes at least one
2 or more alerts related to the user.

1 18. (Original) The method of Claim 16, wherein the signals include multiple alerts
2 generated by multiple users, and the method further comprises correlating the
3 multiple alerts to the multiple users.

1 19-20. (Canceled)

1 21. (Previously Presented) The method of Claim 16 further comprising receiving
2 signals related to an external source including an alert assessment relevant to the
3 network as a whole, wherein the current alert level is also based on the alert
4 assessment.

1 22. (Original) The method of Claim 16 further comprising receiving signals carrying
2 performance information related to a health level of the network, wherein the course
3 of action is based on the set of data and the performance information.

1 24. (Original) The method of Claim 23 further comprising:
2 receiving signals related to one or more alerts;
3 including at least the one or more alerts within a historical dataset of alert related
4 information that establishes a user risk level for a user; and
5 including at least the one or more alerts within a current alert dataset that establishes a
6 current alert level.

1 25. (Original) The method of Claim 23, wherein the sending step further comprising
2 the steps of:
3 deciding on a course of action based on at least a user risk level, a current alert level,
4 and the overall network health level, and

5 the information affecting the use of the network includes at least information for
6 carrying out the course of action.

1 26. (Previously Presented) The method of Claim 25, wherein the deciding step
2 includes at least the steps of:
3 determining the user risk level;
4 determining the current alert level; and
5 determining the overall network health level;
6 wherein the information affecting the use of the network is based on at least the
7 user risk level, the current alert level, and the overall network health level.

1 27. (Currently Amended) A method of policy-based network security management,
2 comprising the computer-implemented steps of:
3 collecting network performance statistics related to an overall health of a network
4 and individual performance statistics of one or more individual units of the
5 network, the collecting being performed by a performance management
6 system;
7 sending the network performance statistics to a controller for analysis;
8 computing an overall health state based on the network performance statistics and
9 the individual performance statistics, using the controller;
10 reading external alert data from an external alert source, using the controller;
11 collecting security event data from the network;
12 sending the security event data to a fault management system;
13 using the fault management system for checking for duplications in the security
14 event data, and deduplicating duplicate security events in the security
15 event data;
16 calculating an alert state based on the security event data from the fault
17 management system and the external alert data, wherein the alert state is a
18 discrete value representing a current measurement of the likelihood of the
19 network being negatively affected;
20 obtaining user information from a subscriber management system;

21 correlating the security event data from the fault management system with the
22 user information to form correlated security event data;
23 reading external user risk data from an external user risk source into the
24 controller;
25 calculating a user risk state based on the correlated security event data and the
26 external user risk data, using the controller, wherein the user risk state is a
27 discrete value representing a long-term measurement of the likelihood of
28 the network being harmed;
29 calculating a decision regarding whether to take corrective action based on the
30 overall health state, the alert state, and the user risk state, using the
31 controller;
32 sending the decision from the controller to the subscriber management system;
33 and
34 sending directives, related to the decision, from the subscriber management
35 system to the network.

1 28. (Currently Amended) A system comprising:
2 a fault management system that receives network security data and deduplicates
3 duplicate indications of security events in the network security data to form
4 deduplicated security event data;
5 a subscriber management system that manages subscribers using a network, wherein
6 the subscriber management system stores subscriber information about
7 individual users and is capable of sending directives to the individual users
8 based on a decision to take corrective action toward the individual users;
9 wherein the deduplicated security event data from the fault management system is
10 correlated to the subscriber information to form correlated network security
11 data;
12 a performance management system that receives overall performance data related to
13 an overall health of the network and individual performance data related to a
14 health of one or more individual units of the network; and
15 a controller that:

16 receives external alert data from an external alert source, external user risk
17 data from an external user risk source, the deduplicated security event
18 data, the correlated network security data, the overall performance
19 data, and the individual performance data;
20 computes an alert state based on at least the external alert data and the
21 deduplicated security event data, wherein the alert state is a discrete
22 value representing a current measurement of the likelihood of the
23 network being negatively affected;
24 computes a user risk state based on at least the external user risk data and the
25 correlated network security data, wherein the user risk state is a
26 discrete value representing a long-term measurement of the likelihood
27 of the network being harmed; and
28 computes a health state based on at least the overall performance data and the
29 individual performance data;
30 makes the decision whether to take corrective action based on at least the alert
31 state, the user risk state, and the health state; and
32 causes directives that implement the decision to be sent to the network.

1 29. (Currently Amended) An apparatus for providing policy-based network security
2 management, comprising:
3 means for receiving a set of data regarding a user of a network, wherein the set of
4 data is a first set of data that is collected over a first duration of time;
5 means for receiving a second set of data that is collected over a second duration of
6 time, wherein the first duration of time is shorter than the second duration of
7 time;
8 means for assessing creating and storing a risk level of the user harming the network
9 based on the second set of data, wherein the second duration of time is
10 sufficient to collect historical data regarding past malicious activities of the
11 user, and wherein the risk level is a discrete value representing a long-term
12 measurement of the likelihood of the user harming the network;

13 means for assessing creating and storing a current alert level based on the first set of
14 data, wherein the first duration of time is of a length appropriate for assessing
15 current activities of the user, and wherein the current alert level is a discrete
16 value representing a current measurement of the likelihood of the user
17 negatively affecting the network;
18 means for automatically deciding on a course of action based on at least one of the
19 risk level and the current alert level, wherein the course of action may be
20 adverse to the user although the current alert level is insufficient to establish
21 whether the user is performing a malicious action; and
22 means for sending signals to one or more network elements in the network to
23 implement the course of action.

1 30. (Currently Amended) An apparatus for providing policy-based network security
2 management, comprising:
3 means for receiving signals carrying network performance information regarding
4 health of a network and resource performance information regarding health of
5 resources used by the network;
6 means for assessing a health level based on the network performance information and
7 the resource performance information;
8 wherein the network performance information, on which the health level is based,
9 comprises at least one of packet latency information, jitter information, packet
10 loss probability (PLP) information, network throughput information, average
11 network downtime information, mean time to repair information, and mean
12 time between failure information;
13 wherein the resource performance information, on which the health level is based,
14 comprises at least one of DHCP server utilization information and ARP table
15 utilization information; and
16 means for sending signals carrying information affecting use of the network based on
17 at least the health level.